IT Professional Technical Services
Master Contract Program - 902TS

Statement of Work (SOW)
For Technology Services
Issued By

Minnesota Department of
Employment and Economic Development (DEED)

Project Title: Web Application Security Assessment (rev.1)

Service Category
Architecture Planning & Assessment – Security and Risk Assessment.

Business Need
The Minnesota Department of Employee and Economic Development (DEED) is the state's principal economic development agency. DEED programs promote business recruitment, expansion, and retention; international trade; workforce development; and community development. DEED has a project currently underway to document all of the applications and their related servers and databases. As part of this effort DEED is looking to strengthen the security of the environment and the applications to protect the Personally Identifiable Information (PII). DEED has approximately 66 applications.

In an effort to strengthen the security of the DEED electronic data stored or processed in multiple tiered applications through-out the department, DEED is requiring an in-depth assessment and analysis of the current security controls in place to protect the confidentiality, integrity and availability (CIA) of critical data and applications. This effort will scrutinize and identify gaps in the controls designed to protect the department's data as well as provide recommendations on improvements to these controls.

We are seeking professional/technical services to independently evaluate the controls protecting PII – see page 7. The applications will need to be classified based on CIA of the data. Using these classifications, define a standard set of expected controls for the identified tiers based on various best practices for information security. The controls identified will then be assessed to identify control deficiencies as well as remediation recommendations to strengthen the security controls to the appropriate level based on the data classification. The assessment results will be used to identify and prioritize remediation activities to strengthen data security.

Once an assessment of the security controls is complete, a test (or vulnerability assessment) will be completed to verify that the security controls are performed as anticipated and identify vulnerabilities. This assessment will provide DEED an accurate picture of the security controls that safeguard the IT application and data. The results of the testing will be used to identify gaps in implemented controls that may expose the applications to security threats. Prioritization and recommendations for remediating the threats and vulnerabilities will be provided to provide input for future IT strategy considerations.

The final phase of this project will perform an application vulnerability assessment of a select set of DEED critical web-based applications to identify vulnerabilities. The objective of this test will be to determine if critical web-based applications are vulnerable to an actionable application-level attack from an external attacker. The application vulnerability assessment should consider OWASP top 10 vulnerabilities.

The anticipated deliverable of the application vulnerability assessment should be a report that documents the web application's existing security posture, identifies specific weaknesses and vulnerabilities, provide examples or descriptions of how vulnerability could be exploited and recommendations to strengthen security at the application level.

By performing these projects, DEED will establish appropriate controls for any application based on its data classification as well as enable the department to provide adequate safeguards for protecting customer's private information. In addition, perform mainframe security assessments and create final report on findings to include mitigation recommendations. Create professional security educational material pamphlet template for employees, managers and visitors.

Project Deliverables - Vendor is expected to create specific technical implementation controls, mitigation activities and documentation for DEED-wide with specific emphasis OLA DEED audit findings starting from phase I through IV below.

I. ***Application Classification and Risk Assessment (All DEED Enterprise Applications)***

a) Classify applications based on criticality of confidentiality, integrity and availability (C.I.A.) requirements within a formal document
b) Define a standard set of expected controls for the identified data classification tiers
c) Assess the identified controls per application
   i) Control Gap Assessment identifying deficiencies
   ii) Control Recommendations to strengthen to an appropriate level based on the type of data stored or accessed
   iii) Data collected must be in an excel formatted file, DEED database, and be made available in DEED's SharePoint collaboration site
   iv) Identify business owner and IT representative

II. ***Vulnerability Assessment of DEED IT Environment (All DEED Enterprise Applications Containing PII)***

a) Perform a test of the implemented controls of the IT environment surrounding the department's applications within a formal document
   i) Identify gaps in implemented controls that may expose the application and data to security threats
      (1) Conduct external and internal scanning and configuration reviews of DEED technology assets
      (2) Create a prioritized list of technical vulnerabilities (internal and external) prioritized by "risk factor" (probability x impact rating)
      (3) Analysis summary of the top root causes for vulnerabilities
      (4) Provide recommendations for remediation
      (5) Data collected must be in an excel formatted file, DEED database, and be made available in DEED's SharePoint collaboration site
      (6) Data collected must link directly to the application resource allocation project which identifies location of all enterprise applications on servers

III. ***Application Vulnerability Assessment (All DEED Enterprise Applications Containing PII)***

a) Interrogate the web applications for vulnerabilities within a formal document
   i) Summary of the scope and processes tested
   ii) Detailed findings on vulnerabilities discovered including a narrative of the process to be able to conduct an exploit **per each application**
   iii) Recommendations for remediation including reference to Open Web Application Security Project (OWASP) best practices for application development **per each application**

iv) Data collected must be in an excel formatted file, DEED database, and be made available in DEED's SharePoint collaboration site

IV. *Mainframe and Security Awareness Material*

a) Perform mainframe security assessments and create final report on findings to include mitigation recommendations
b) Create professional security educational material pamphlet template for employees, managers and visitors. Describe security roles, responsibilities to protect and safeguard DEED information

Contract Type

The Web Application Security Assessment project will be completed under a fixed bid contract.

Project Schedule

We anticipate this project will start on or about **Tuesday**, **September 7, 2010**. Project end date will depend on vendor proposals. A DEED project manager will be assigned to perform work on each security control.

Agency Project Requirements

- Work will be completed at DEED's First National Bank offices in St. Paul, MN between normal business hours of 8:00 am to 5:00 pm, excluding holidays.

Responsibilities Expected of the Selected Vendor

- Hire appropriate person with specific OWASP best practices and application development \ expertise
- Train and transfer knowledge to DED employees

Required Skills (These are to be scored as pass/fail requirements)

- 4 years' or more experience performing application classification, risk management, vulnerability assessments and application vulnerability assessment
- 4 years' experience within Information Technology

Desired Skills

- Two or more engagements which demonstrates communication and collaboration across a variety of audiences, including business people and technologists
- Three or more years demonstrated technical expertise in web application security as based on interview and resume
- Excellent verbal and written communication skills based upon interview
- One or more security engagements with Minnesota State systems
- Vendor will have the required NIST knowledge

Process Schedule

Deadline for Questions	***Friday, August 20, 2010, 4:00 PM, CDT***
Posted Response to Questions	***Tuesday, August 24, 2010, 3:00 PM, CDT***
Proposals due	***Friday, August 27, 2010, 3:00 PM, CDT***
Anticipated proposal evaluation begins	***Monday, August 30, 2010***
Potential vendor interviews	***Tuesday, September 1 – 3, 2010***
Anticipated decision	***Friday, September 4, 2010***

Questions

Any questions regarding this Statement of Work should be submitted via e-mail or hand carried by the process schedule deadline for questions to: Reginald Williams, DEED Chief Information Security Officer.

E-mail Address: Reginald.williams@state.mn.us

Other persons ARE NOT authorized to discuss this SOW or its requirements with anyone throughout the selection process and responders should not rely on information obtained from non-authorized individuals. If it is discovered a Responder contacted other State staff other than the individual above, the responder's proposal may be removed from further consideration.

SOW Evaluation Process

Each section of the vendor responses will be evaluated / scored by an evaluation team of DEED employees.

Step 1: Pass/Fail Criteria. Review responses to ensure proposals meet pass/fail criteria before further consideration/evaluation is completed.

Step 2: All proposals that meet the requirements of Step 1 will be evaluated based on the weighting factors listed below:

- Experience (required skills) (25%)
- Desired skills (20%)
- Proposed Work Plan (25%)
- Cost (30%)

Step 3: Interviews – DEED at their discretion, may conduct interviews with the top-scoring vendors as part of the final selection process.

The next section will point out more clearly how responses should be formatted and how they will be scored.

Response Requirements

Vendor will provide the applicable and necessary labor, supervision, consultation, and/or tools to perform the Services and provide the Deliverables described in this SOW.

For purposes of this SOW, "Deliverables" means any materials produced in the course of performing Services listed or specifically required to be delivered to Client under this SOW.

Please adhere to noted page limits. Failure to do so may result in a material failure of the proposal and the vendor's proposal may be taken out of consideration. Font should be no smaller than 10 pt and pages should have 1" margins on all sides.

Section 1: Cover page with only the following information (limit one page):

Vendor Company Name
Address
City, State, Zip
Company Contact Person
Contact person's email and phone information

Resource Name #1 and 2

Section 2: Deliverables: Vendor will provide the following Deliverables:

a. Identify resumes for consultant(s) working for vendor. Resume should not be more than 3 pages long related to applicable experience.

b. Supply previous client engagement information related to application classification and risk assessments, vulnerability assessment and application vulnerability assessment documents, also please expunge prior client's and sensitive information.

c. Provide two recommendations on application classification and risk assessment. The recommendations should include name, title and phone numbers.

d. Project Plan. Vendor will provide an estimate of a draft project plan for phase 1 through IV.

Section 3 – Cost – detailed cost proposal included the following:

a. Total Project Cost – Include breakdown costs for Phase I through IV and then complete totals.

b. Project Management (PM) Cost – minimal project management and minor administrative support hours is required to initiate and follow-up on meetings with key stakeholders, business representatives, CISO, application developers, directors and managers. PM will ensure specific deliverables are timely and complete through the CISO. However, DEED BIT reserves the right to perform project management activities.

c. Hourly rate and total estimated hours for each staff member you intend to assign to the project. Hourly rates cannot exceed the hourly rate identified in your 902TS master contract for the OET service category indicated in this Statement of Work and/or Work Plan categories identified as part of Vendor Response. This estimated timeframe is based upon Client providing unrestricted access to internal experts, location(s), all critical systems, applications, and hardware required to complete project.

Section 4: State Forms - Required forms to be returned or additional provisions that must be included in proposal. See General Requirements Section below for more information.

a) Conflict of Interest Statement
A statement certifying there are no known conflicts of interest with respect to this project, or if known, identification of those situations that may present an actual or potential conflict and how the contractor proposes to avoid the potential conflict.

b) Affirmative Action Certificate of Compliance
http://www.mmd.admin.state.mn.us/doc/affaction.doc

c) Affidavit of non-collusion
http://www.mmd.admin.state.mn.us/doc/noncollusion.doc

d) Immigration Status Certification
http://www.mmd.admin.state.mn.us/doc/immstatcert.doc

e) Location of Service Disclosure
http://www.mmd.admin.state.mn.us/Doc/ForeignOutsourcingDisclosureCertification.doc

f) Certification Regarding Lobbying
http://www.mmd.admin.state.mn.us/doc/lobbying.doc

g) Veteran-Owned/Service Disabled Veteran-Owned Preference Form
http://www.mmd.admin.state.mn.us/doc/vetpref.doc

Response Submission Instructions

- Sealed responses must be received at the following address no later than the process dates for sealed responses and should be addressed to:

  Security Web Application Assessment
  Attn: Reginald Williams, DEED CISO
  Minnesota Department of Employment and Economic Development
  1st National Bank Building
  332 Minnesota St., Suite E200
  St. Paul, MN 55101

- All proposals will be time and date stamped when they are received. Proposals received after the deadline will not be considered and will be returned unopened to the responder. Emailed responses will NOT be considered.

- Please submit 2 copies of Sections 1, 2 & 3. You need only submit **one copy** of Section 4: State Forms

- DO NOT include marketing materials or any other information not requested in Response Requirements.

- DEED will NOT be conducting a reverse auction for this SOW.

General Requirements to Understand Before Submitting a Response

Proposal Contents

By submission of a proposal, Responder warrants that the information provided is true, correct and reliable for purposes of evaluation for potential award of this work order. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the responder to suspension or debarment proceedings as well as other remedies available by law.

Liability

The Contractor must indemnify, save, and hold the State, its agents, and employees harmless from any claims or causes of action, including attorney's fees incurred by the State, arising from the performance of this contract by the Contractor or the Contractor's agents or employees. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligations under this contract.

Disposition of Responses

All materials submitted in response to this SOW will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the selected vendor. If the Responder submits information in response to this SOW that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, the Responder must: clearly mark all trade secret materials in its response at the time the response is submitted, include a statement with its response justifying the trade secret designation for each item, and defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments or damages awarded against the State in favor of the party requesting

the materials, and any and all costs connected with that defense. This indemnification survives the State's award of a contract. In submitting a response to this SOW, the Responder agrees that this indemnification survives as long as the trade secret materials are in possession of the State.

The State will not consider the prices submitted by the Responder to be proprietary or trade secret materials.

Conflicts of Interest

Responder must provide a list of all entities with which it has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request for proposals. The list should indicate the name of the entity, the relationship, and a discussion of the conflict.

The responder warrants that, to the best of its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to organizational conflicts of interest.

An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons, a vendor is unable or potentially unable to render impartial assistance or advice to the State, or the vendor's objectivity in performing the contract work is or might be otherwise impaired, or the vendor has an unfair competitive advantage.
The responder agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to the Assistant Director of the Department of Administration's Materials Management Division ("MMD") which must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organization conflict of interest is determined to exist, the State may, at its discretion, cancel the contract. In the event the responder was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to MMD, the State may terminate the contract for default. The provisions of this clause must be included in all subcontracts for work to be performed similar to the service provided by the prime contractor, and the terms "contract," "contractor," and "contracting officer" modified appropriately to preserve the State's rights.

Preference to Targeted Group and Economically Disadvantaged Business and Individuals

In accordance with Minnesota Rules, part 1230.1810, subpart B and Minnesota Rules, part 1230.1830, certified Targeted Group Businesses and individuals submitting proposals as prime contractors shall receive the equivalent of a six percent preference in the evaluation of their proposal, and certified Economically Disadvantaged Businesses and individuals submitting proposals as prime contractors shall receive the equivalent of a six percent preference in the evaluation of their proposal. Eligible TG businesses must be currently certified by the Materials Management Division prior to the solicitation opening date and time. For information regarding certification, contact the Materials Management Helpline at 651.296.2600, or you may reach the Helpline by email at mmdhelp.line@state.mn.us. For TTY/TDD communications, contact the Helpline through the Minnesota Relay Services at 1.800.627.3529.

Veteran-owned/Service Disabled Veteran-Owned Preference

In accordance with Laws of Minnesota, 2009, Chapter 101, Article 2, Section 56, eligible certified veteran-owned and eligible certified service-disabled veteran-owned small businesses will receive a 6 percent preference in the evaluation of their proposal.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses should complete the Veteran-Owned/Service Disabled Veteran-Owned Preference Form in this solicitation, and include the required documentation. Only eligible, certified, veteran-owned/service disabled small businesses that provide the required documentation, per the form, will be given the preference.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses must be currently certified by the U.S. Department of Veterans Affairs prior to the solicitation opening date and time to

receive the preference.

Information regarding certification by the United States Department of Veterans Affairs may be found at http://www.vetbiz.gov.

Foreign Outsourcing of Work Prohibited

All services under this contract shall be performed within the borders of the United States. All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by subcontractors at all tiers.

Statement of Work does not obligate the state to award a work order or complete the assignment, and the state reserves the right to cancel the solicitation if it is considered to be in its best interest. The Agency reserves the right to reject any and all proposals.

Definition:

Personable Identifiable Information (PII) is ―any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.‖ [6] Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother‘s maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver‘s license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).